Hitachi ID Identity Express™ - Corporate Edition

hitachi-id.com

Challenges

Complex Process Implementation

IAM systems automate business processes by granting access to joiners, adjusting access for movers, revoking the access of leavers. These processes are complex: unreliable data spread across multiple systems of record, redundant requests for the same user/access, data archiving post termination, reversing improper changes and more. This complexity contributes to cost, risk and delay in IAM processing.

Replacing Legacy Processes

The cost, risk and delay of automating complex processes can be mitigated by replacing sub-optimal legacy processes with a proven, standardized system.

Governance Automation

The largest security benefit from IAM automation is to deactivate access for leavers. The largest ROI comes from granting access more quickly and reducing the number of people managing access. A focus on access certification and "data cleanup" ahead of process automation defers these benefits for years, in favour of cleaning entitlements in spreadsheets.

Key Benefits

Hitachi ID Identity Express -- Corporate Edition encapsulates best practices business processes for joiner, mover and leaver processes, as well as policy controls governing access and privacy. Organizations that deploy Identity Express benefit from rapid, low-cost, low-risk process automation while improving requester usability, service responsiveness and controls.

Best Practices IAM Process Automation

Hitachi ID Identity Express -- Corporate Edition implements pre-configured best practices to automate user lifecycles and entitlements.

Automatically Grant and Revoke Employee Access

Identity Express monitors one or more systems of record (typically HR applications) and detects changes. It automatically creates new user profiles and accounts for new employees and deactivates access when users leave.

Request Portal for Contractors

Identity Express includes request forms for onboarding and deactivating contractors, vendors and other classes of users, typically generated by the HR system.

Day-one Initiation

New hires access self-service password reset on their first day, authenticating by answering Personally Identifiable Information (PII) questions and/or entering a PIN sent to their mobile. They must read and accept policy documents and answer security questions before setting their initial password.

Multi-step Access Deactivation

Identity Express supports both urgent and scheduled user deactivation. Managers are notified in advance and can reschedule departure dates. Access is automatically disabled and can be reactivated if required. Home directories and mail folders are archived and identity data is retained to support audits and rehire detection.

Leaves of Absence

Identity Express supports leaves of absence (LoA). An LoA may be initiated or ended either immediately or on a scheduled date. If users on LoA do not return, they can be marked as terminated.

Access Requests

Identity Express supports three mechanisms to request new access rights: search for the required entitlement; compare the entitlements or intercept an "Access Denied" error on Windows or SharePoint. Requests may be self-service or submitted by one user on behalf of another.

Hitachi ID Systems, Inc.

HITACHI
Inspire the Next

Access Control and Privacy Protection

User access data is strictly controlled, limiting what peers of a given user can search for and what data is visible or changeable. All access rights are linked to the relationship between requester and recipient -- for example manager/subordinate or HR/employee.

Robust Workflow

Users may be invited to authorize, review or implement access change processes. A robust workflow engine can invite multiple users concurrently, send reminders, escalate unresponsive participants, schedule time off and more. Authorizers can approve or reject using their phones, even without a public URL to the system.

User Moves and Name Changes

Included forms and HR integration support name changes and updates by the user's manager. These changes may trigger the assignment of a new login ID or e-mail address or moving the user's home directory or mailbox to a new server.

Access Reviews / Certification

Identity Express supports both periodic and event-triggered access reviews. The reporting relationships and access rights of users are presented to stake-holders, to either certify or mark as inappropriate.

Included Connectors

Directory

Windows/Active Directory, LDAP, eDirectory, NDS

File/Print

Windows, NetWare, Samba, NAS appliances

Database

Oracle, Sybase, SQL Server, DB2/UDB

Unix

Linux, Solaris, AIX, HP-US with passwd, shadow, TCB, Kerberos, NIS or NIS+

Mainframes/Mini

z/OS with RACF, TopSecret or ACF/2, iSeries, Scripts for VM/ESA, Unisys, Siemens, OpenVMS, Tandem

Application

Oracle eBiz, PeopleSoft, SAP R/3, JDE and more

Groupware

Exchange 2000-2010, Notes NAB and ID files, GroupWise

Networking

Networking devices and VPNs via AD, LDAP, SSH

Cloud/SaaS

WebEx Connect, Google Apps, Salesforce.com, UltiPro HR, Office 365, Cybershift

Hitachi ID Identity Express - Corporate Edition is a set of pre-configured business processes and policies built on top of Hitachi ID Identity Manager and Hitachi ID Password Manager. It embodies best practices for managing the identities, entitlements and credentials of employees and contractors in a corporate organization.

For more information, please visit: http://hitachi-id.com/
or call: 1.403.233.0740 | 1.877.386.0372

HITACHI
Inspire the Next